using a calculated hash (T1)

L3: Entry 1 of 3 File: USPT Feb 22, 2005

DOCUMENT-IDENTIFIER: US 6859790 B1
TITLE: Data distribution system and method thereof, data processing device, data control device, and machine-readable recording medium recording distribution data

Detailed Description Text (167):
Then, the value obtained by passing the current value through the hash function once each time the user makes a copy is compared with the permitted number of generations, confirmation is made regarding whether or not this has exceeded the purchased number of tickets, and if not so, the copy action is permitted.

Detailed Description Text (173):
At the time of copying to the media B, the current value T(0) described to the usage state (status) is passed through the hash function once to obtain the current value T(1). Next, in the event that comparison is made with the number of permitted generations T(4) described in the conditions of use (policy) and confirmation is made that this has not been exceeded, copying is carried out. Then, the current state of the usage state (status) of the media A is updated with the new current value T(1), and this is recorded to the usage state (status) of the media B as the current value of the media B. Also, this T(1) is recorded to the usage state (status) as the number of permitted generations of the media B, as well. Accordingly, at this point, the media B is set at number of permitted generations=current value, so the number of recording tickets is zero.

CLAIMS:

10. A data distribution method, which: adds to desired contents data, in a manner wherein external operation is impossible, use control information containing information of the number of permitted times of use, which is the number of times that use of said contents data including either one or both of recording and playing said contents data is to be permitted, and generates distribution data; distributes said distribution data to a desired distribution destination; detects whether or not the use of said contents data of said distribution data is permitted, based on said use control information of said distributed distribution data, at said distribution destination; uses said contents data in the event that use thereof is permitted as the result of said detection; and updates said use control information so as to decrease said number of permitted times of use according to said usage; wherein detection of whether or not use of said contents data is permitted, control of use of said contents data based on said detection results, and updating of said use control information based on said use, are performed within a signal processing device regarding which external observation and alteration of the signal processing state is impossible; wherein in the event that said contents data has been used, said distribution destination sends information relating to use of said contents data to a predetermined administration device; wherein said administration device performs billing processing relating to use of said contents data, based on said generated information relating to use of said contents data; and wherein in the event of using said contents data by recording, this is performed by using as a unit; said distribution data containing said contents data and said use control information containing said information of the number of permitted times of use that has been newly set; wherein said distribution data contains information of the number of times use has been

permitted and the number of times essentially already used, as said use control information, with a hash value of a hash function; and wherein detection of whether or not use of said distribution data is permitted, and updating of information indicating the number of times said distribution data has already been essentially used based on use of said distribution data, are performed by comparing information of said number of permitted times of use with information of number of times already used, at said distribution destination.

Previous Doc Next Doc Go to Doc#

L3: Entry 2 of 3 File: USPT Jul 29, 2003

DOCUMENT-IDENTIFIER: US 6601046 B1
TITLE: Usage dependent ticket to protect copy-protected material

Detailed Description Text (10):
Other security techniques, common in the art, may also be applied. Illustrated in FIG. 1, the playback device 300 includes a ticket extractor 330 and watermark extractor 340. Generally, a watermark is a characteristic that is embedded within content. material such that a removal of the watermark cannot be effected without destroying or substantially degrading the content material. As presented in copending U.S. patent application, "Copy Protection by Ticket Encryption", Ser. No. 09/333,628, filed Jun. 15, 1999 for Michael A. Epstein, incorporated by reference herein, a ticket that controls access rights to the content material can be associated with the watermark, typically via a one-way hashing function. Rules are provided for determining the validity of the ticket, based on a comparison with a hashed, or multiply hashed, value of the watermark. If the content material 125' contains a watermark but does not contain a valid ticket, the authorization device 360 prohibits its rendering 361, regardless of the validity of the above described usage measures. In this manner, illicitly obtained content material 125 cannot be recorded onto recording media 200 that contain valid usage measures and parameters. To further prevent substitute content material 125 being illicitly recorded onto media 200 containing valid usage measures and parameters, a preferred embodiment of this invention binds the baseline-usage parameters 145 to the content material for which the portion of the total-usage measure was allocated. For example, the aforementioned ticket can be included in the baseline-usage parameters 145 that are encrypted or digitally signed before loading into the baseline-usage register 230 of the recording medium 200. An attempted counterfeit substitution of the ticket or the content material, or both, will result in a rejection by the authorization device 360 in conjunction with the security device 350. A substituted ticket will fail the aforementioned verification test based on the public key of the trusted provider, whether it matches the counterfeit content material or not, and a substituted counterfeit content material will not match a verified ticket that is associated with the original content material.

L3: Entry 3 of 3 File: USPT Dec 24, 2002

DOCUMENT-IDENTIFIER: US 6499105 B1
TITLE: Digital data authentication method

Detailed Description Text (27):
Next, the controlling module 112 tells the signature verifying module 114 to verify the digital signature (step 602). To do so, the signature verifying module 114 decrypts the extracted digital signature using the verification key 122 of a user stored in the storage module 120 and compares the resulting value with the hash value obtained by evaluating the original content in the storage module 120 with the use of the same one-way hash function as that used by the purchaser system 200. If the rule used by the purchaser system 200 to embed the digital signature into the content is known only to the provider and if the digital signature may be removed from the content according to that rule, the content from which the digital signature is removed may be used instead of the original content.

Detailed Description Text (196):
That is, as shown in FIG. 24, the terminal 1101 first extracts a mark 2407 from a Web page 2406 to check its validity (step 2401) and extracts a hash value 2408 embedded in the extracted mark 2407 as a digital watermark (step 2402). The terminal 1101 also calculates a hash value 2409 of the Web page data except the part related to the mark whose validity is to be checked (step 2403) and compares the calculated hash value 2409 with the hash value 2408 extracted from the mark (step 2404). If they match, the terminal 1101 displays a message stating that the mark was validated on the display unit 1102; if they do not match, the terminal 1101 displays a message stating that the mark was not validated on the display unit 1102 (step 2405).

Detailed Description Text (212):
That is, as shown in FIG. 29, the terminal 1800a first gets a public key 2910 of the mark management organization 1121 from the public key DB 1801. Then, the terminal 1800a extracts a mark 2908 from a Web page 2907 to check its validity (step 2901), extracts a digital signature 2909 embedded in the extracted mark 2908 as a digital watermark (step 2902), and decrypts the extracted digital signature using the public key 2910 of the mark management organization 1121 to get a hash value 2911 (step 2903). The terminal 1800a also calculates a hash value 2912 of the Web page data except the part related to the mark 2908 whose validity is to be checked (step 2904), and compares the calculated hash value 2912 with the hash value 2911 generated by decrypting the digital signature extracted from the mark 2908 (step 2905). If they match, the terminal 1800a displays a message on the display unit 1102 stating that the mark was validated; if they do not match, the terminal 1800a displays a message staging that the mark was not validated (step 2906).

Detailed Description Text (219):
That is, in the sixth embodiment, the consumer terminal extracts the mark to be validated from the Web page, and sends the extracted mark and a validity check request to the mark management server. In the seventh and eighth embodiments, the consumer terminal sends Web page data containing the mark and the validity check

request to the mark management server. On the display unit of the consumer terminal there is displayed a successful or an unsuccessful validity check message sent back from the mark management server. On the other hand, upon receiving a validity check request, the mark management server performs the validity check on the mark in the same way as the consumer terminal performs in the sixth to eighth embodiments. In the sixth embodiment, the mark management server extracts information embedded in the mark sent with the request. If this information matches the information embedded by the mark management server, it sends a successful validity message to the consumer terminal; if not, it sends an unsuccessful validity check message to the consumer terminal. In the seventh embodiment, the mark management server extracts the mark from the Web page sent with the request, extracts the hash value embedded in the mark as the digital watermark, calculates the hash value of the Web page except the area related to the mark to be validated, and compares this value with the hash value extracted from the mark. If they match, the mark management server sends a successful validity check message to the consumer terminal, and if not, it sends an unsuccessful message to the consumer terminal. In the eighth embodiment, the mark management server extracts the mark from the Web page sent with the request, extracts the digital signature embedded in the extracted mark as the digital watermark, and extracts the hash value by decrypting the digital signature with a public key of the mark management organization. The mark management server calculates the hash value of the Web page data except the area related to the mark to be validated, and compares this value with the hash value generated by decrypting the digital signature extracted from the mark. If they match, the mark management server sends a successful validity check message to the consumer terminal, and if not, it sends an unsuccessful message to the consumer terminal.

Previous Doc Next Doc Go to Doc#